SANS Internet Storm Center

Johannes Ullrich, Ph.D.
Chief Research Officer
SANS Institute

Outline

- Internet Storm Center and DShield
- Global Collaborative Incident Handling: DNS Poisoning.
- Outlook / Future Threats
- Q & A

Internet Storm Center & DShield

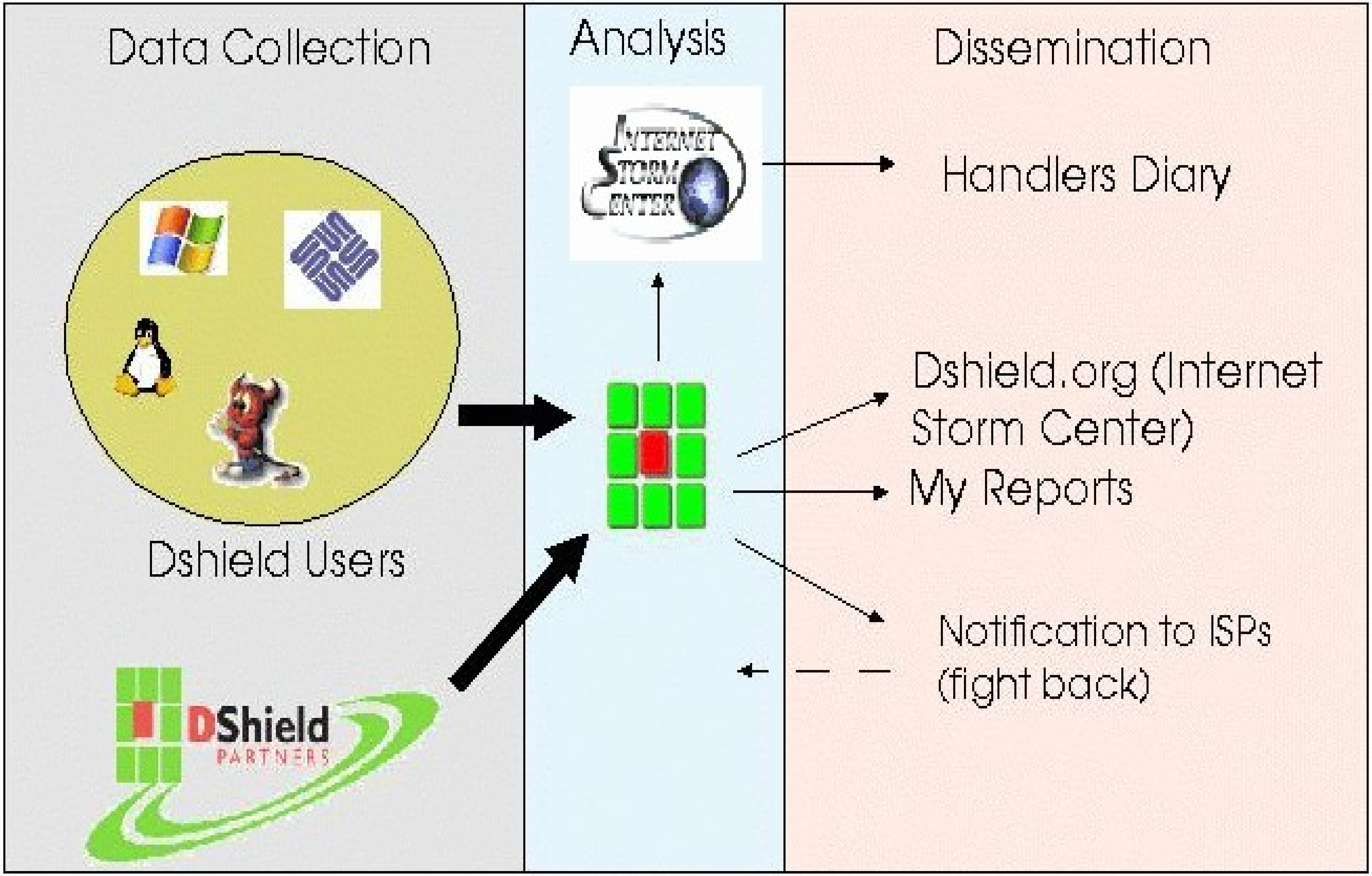
- http://www.dshield.org
- Large global firewall log database.
- Automated data collection and reporting.
- Tool to detect long term trends as well as fast moving outbreaks.

- http://isc.sans.org
- Used to disseminate results and collect individual reports.
- Analysis of reports (from ISC readers as well as DShield) performed by 40 volunteer “handlers”.

DShield.org

- Sensors worldwide covering about 500,000 routable IP addresses.
- data load approaching 1 Billion reports / month.
- We only collect simple header information (source/target IP and port, time stamp, flags...)
- System designed for fast detection of new trends and used as a aid to focus handler's attention to new traffic patterns.

Information Flow



DShield Reports Demo

Public Page:
http://www.dshield.org

Reports for Submitters:

https://secure.dshield.org

e-mail: demo@dshield.org
userid: 11111

Sign Up!

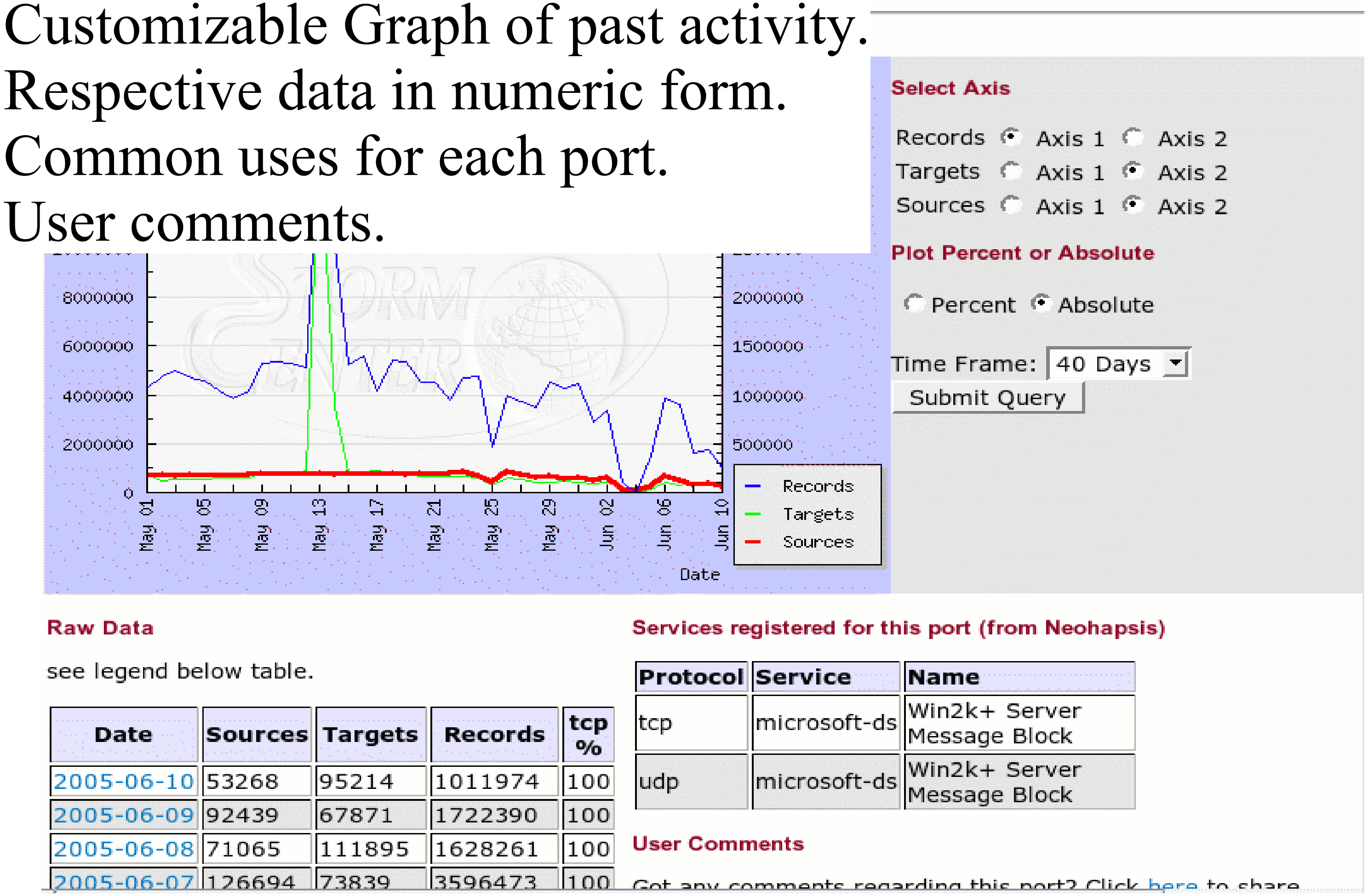
http://www.dshield.org/howto.php

8Signs Firewall Agnitum Outpost AnalogX PortBlocker
Asante FriendlyNET, D-Link, U.S. Robotics, and SMC Barricade routers using RouterLog BlackIce Defender
eSoft Instagate Firewall Kerio (formerly Tiny) Personal Firewall
Kerio (formerly Tiny) Software WinRoute Pro Asante FriendlyNet VR2004AC, VR2004C Billion Bintec
Buffalo Checkpoint VPN-1 Edge Cisco ACL (IOS) Cisco PIX Clavister Firewall D-Link Fortigte Gentek
IPChains IPTables Level One Linksys Router m0n0wall Firewall Netgear Router Netscreen Netopia SMC
Smoothwall Sonicwall WatchGuard Zyxel Zywall Linksys Etherfast Cable / DSL router Microsoft ISA
McAfee Firewall Norton Personal Firewall Snort Sygate Personal Firewall Symantec VelociRaptor Firewall
Tiny Personal Firewall 4.0 and 5.0 Vicom Internet Gateway Trend Micro PC-Cillin
VisNetic (formerlly Ambra) Firewall Wingate Proxy Server Windows XP Internet Connection Firewall (ICF)
ZoneAlarm Cisco PX Firewall DIDSyslog SonicWall Syslog Daemon Link Logger (Linksys,
Prestige/Netgear, and ZyXel ZyWall routers) US Robotics 8000 router
VisualZone Report Utility for ZoneAlarm(ZoneAlarm) Wallwatcher (2Wire, Cisco PIX, D-Link DFL-80, DI-804HV, IPTables, Linksys, Netgear FR114P, Netscreen 5GT, ZyxelP334 routers) Watchguard Firebox
ZoneLog (For ZoneAlarm) Firewalls that send logs by email SonicWall (But see DIDSyslog,above.)
Dlink DI614+ Kernel packet logs as generated by Linux 2.2.x and ipchains
Kernel packet logs as generated by Linux 2.4.x and iptables Checkpoint Firewall-1 User Alerts
Checkpoint Firewall-1 Version 4.1 Cisco ACL Cisco PIX DLink DI-640 Freesco
Foundry Networks ServerIron Kerio (formally Tiny) Firewall Syslog Gauntlet firewall Gnatbox firewall
Linux Etherfast Cable / DSL router Open BSD ipf logs Open BSD Packet Filter logs Psionic Portsentry logs
Snort and Snort Portscan logs Zyxel Prestige 650, 310/314 and Netgear RT310/314
User contributed Linux and UNIX clients ipchains and iptables client written in Python IPCop Firewall LaBrea
Compatible Systems Microrouter Netscreen Firewalls Nexland Router FreeBSD ipf(4) and ipmon(8) logs
IPFW logs Solaris ipf logs Symantec Firewall/VPN Appliance ulogd Watchguard Firebox

Port Info

http://isc.sans.org/port_details.php?port=445

- Customizable Graph of past activity.
- Respective data in numeric form.
- Common uses for each port.
- User comments.



Select Axis

Records ● Axis 1 ○ Axis 2
Targets ○ Axis 1 ● Axis 2
Sources ○ Axis 1 ● Axis 2

Plot Percent or Absolute

○ Percent ● Absolute

Time Frame: 40 Days

Raw Data

see legend below table.

Date	Sources	Targets	Records	tcp %
2005-06-10	53268	95214	1011974	100
2005-06-09	92439	67871	1722390	100
2005-06-08	71065	111895	1628261	100
2005-06-07	126694	73839	3596473	100

Services registered for this port (from Neohapsis)

Protocol	Service	Name
tcp	microsoft-ds	Win2k+ Server Message Block
udp	microsoft-ds	Win2k+ Server Message Block

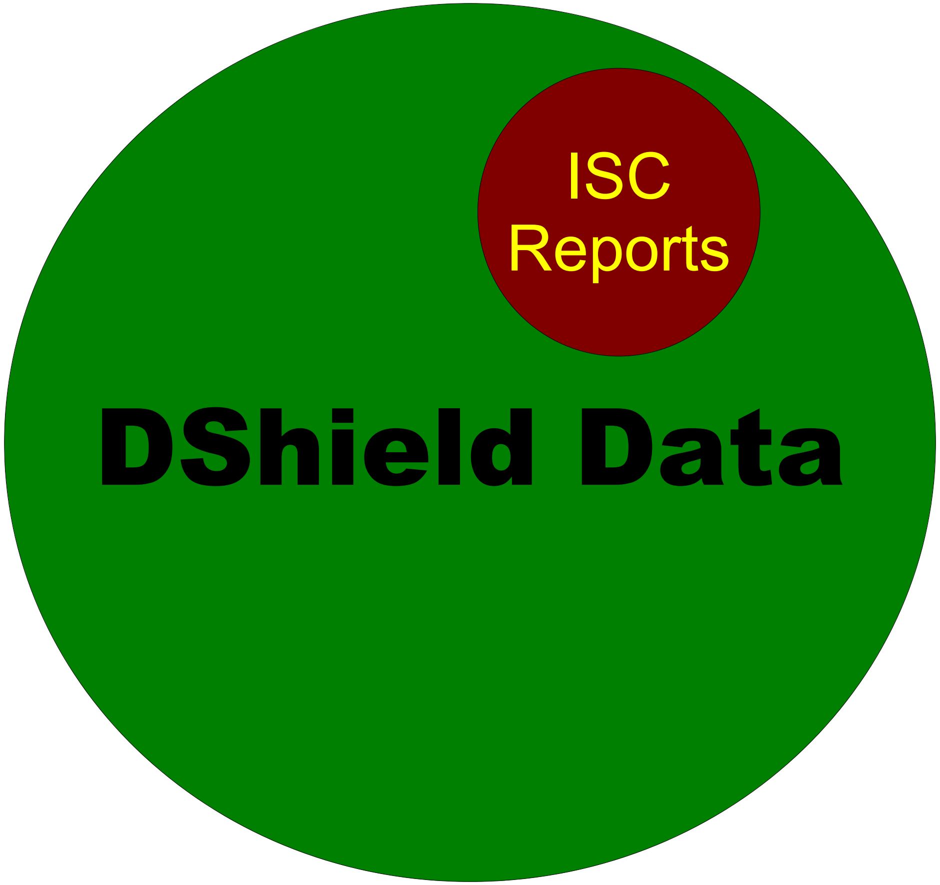
User Comments

Got any comments regarding this port? Click here to share

Internet Storm Center

- 40 “Handlers”
- each day, a particular handler volunteers as “handler of the day”.
- Handler of the day is coordinating response.
- Handlers are selected to represent different industries and geographic areas.
- Information is disseminated expeditiously to not only provide the earliest possible warning, but also to obtain more detailed information from readers.

Incident handling process



Reports from ISC readers are used to explain features found in DShield data. If unexplained features are found, the diary is used to solicit observations from readers.

ISC Features

- Diary
- Top Ports / IPs List
- IP / Port Info
- Some ASN based reports
- Trends
- Contact Form

Diary

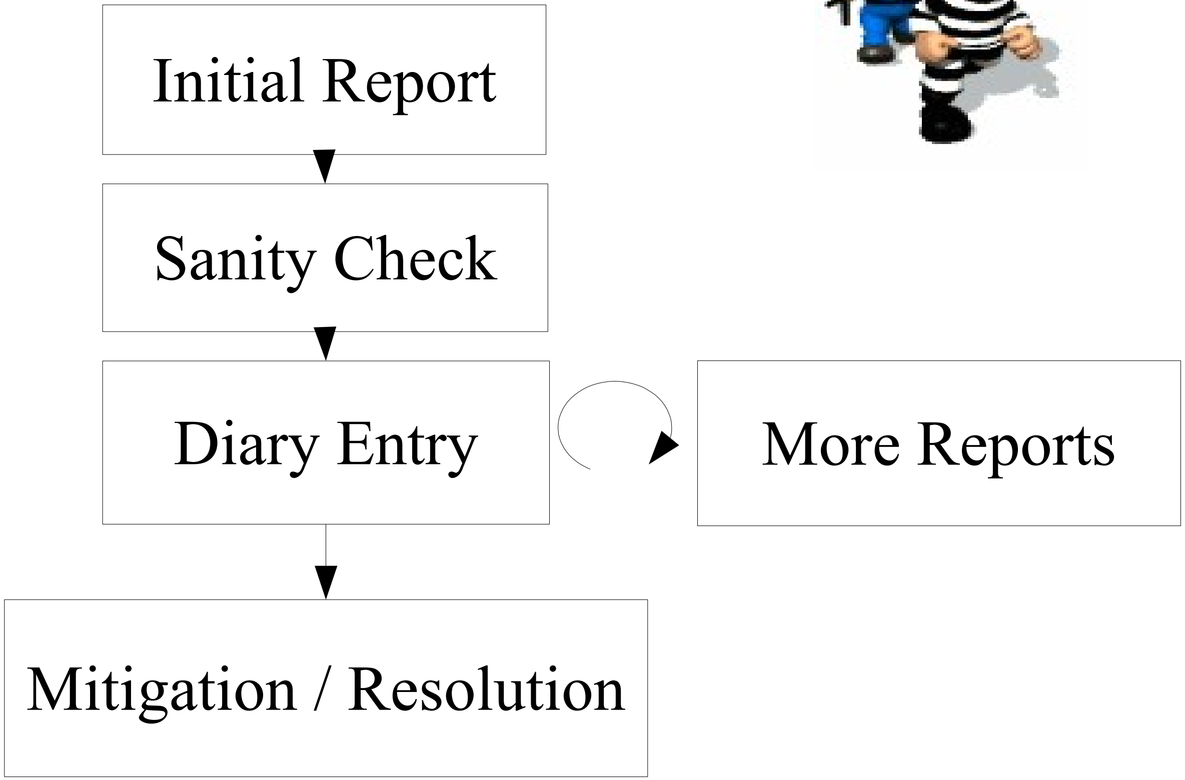
- Written by “Handler of the Day” (HOD).
- Updated at least once a day, more frequently if required.
- Summarizes events reported to ISC.
- NOT a news summary.
- Reflects priorities / opinions of the HOD.
- Usually written with input from other handlers.

GOAL: When reading the diary, you should recognize an event you dealt with that day (or will deal with).

Global Incident Handling

Sample Event: DNS Poisoning.

Basic event handling flow chart:



Initial Report

Sanity Check

Diary Entry

More Reports

Mitigation / Resolution

DNS Poisoning

“We are beginning to see a widespread browser hijacking within our corporate enterprise. ... it has all the looks of a DNS poisoning, but we can't find anything on our INTERNAL network which indicates we have an internal problem. There is no commonality in sites (other than being well known sites), and there is no indication of an internal worm. But the hijack has infected a number of different workstations who didn't access any of the same sites. One example was: get www.weather.com, followed by the get "download" html to the same ip address, then a GET to what appears to be he REAL www.weather.com. Some of the hijacked sites are: www.7sir7.com, www.abx4.com, etc.. This looks like a regular spyware thing, but the problem is is that it's propagated within our enterprise like a worm.

Gary, (March 3rd 2005)

Initial Screening

- “hosts” file? (Gary: no)
- are non-browser DNS lookups (e.g. nslookup) affected? (Gary: nslookup provides bad results)
- Preliminary conclusion: This could be DNS poisoning.
- Action: Add note to diary

Reaction to Diary

Various other reports. Sample:

> Hi SANS! Had an issue today where it appears our DNS cache was poisoned somehow. Alot of sites were being redirected to www.123xxl.com/index2.php. The IP addresses that this was being resolved to were 217.160.169.87, 216.127.88.131, 207.44.240.79. This site then tried to download an Active-X control of some kind. I did not allow it to download, but I was hoping one of you could check it out in a lab to see what it does. I'll continue to research, and let you know if I find out anything.
>
> John (3/3/2005)

Refined response

- Ask users to check DNS cache content.
- Offer help by publishing command lines to dump cache.
- Offer advice about how to flush the cache.
- Request blocking of access to target web servers.
- Users report that problem goes away after cache is cleared.
- IP Address keeps changing
- Malware distributing site associated with 7sir7.com and abx4.com

Symantec Gateway Products

March 4th:

Number of affected users report that they are using Symantec firewall appliances, which provide DNS caching.

Possibly related to vulnerability/patch from June 2004.

March 6th:

Symantec releases a hotfix for its Gateway Security and Enterprise Firewall products.

Additional Reports come in

March 13th:
7sir7 exploit is planted on a large number of sites using exploited "web site motels".

More reports about cache poisoning from sites not using Symantec products.

March 30th:
reports of cache poisoning pick up again.

Sample 'dig' output

```
; <<>> DiG 9.2.4 <<>> www.cnn.com @218.38.13.108
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59667
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1,
ADDITIONAL: 1

;; QUESTION SECTION:
;www.cnn.com.                   IN      A

;; ANSWER SECTION:
www.cnn.com.            99999   IN      A       205.162.201.11
www.cnn.com.            99999   IN      A       217.16.26.148

;; AUTHORITY SECTION:
com.                    99999   IN      NS      besthost.co.kr.

;; ADDITIONAL SECTION:
besthost.co.kr.         1800    IN      A       218.38.13.108

;; Query time: 236 msec
;; SERVER: 218.38.13.108#53(218.38.13.108)
;; WHEN: Thu Mar 31 16:01:07 2005
;; MSG SIZE  rcvd: 105
```

DNS poisoning stats

From a web server that hosted the malware site on March 3rd, we received logs showing the following “success numbers” for this attack:

1,304 different domain names got redirected to the site.
8 Million HTTP GET attempts.
966 unique IP addresses.
75 thousand incoming e-mail messages.
7,500 failed ftp login attempts
7,700 failed imap login attempts
2000 logins to 82 different webmail systems.

Moving to Yellow

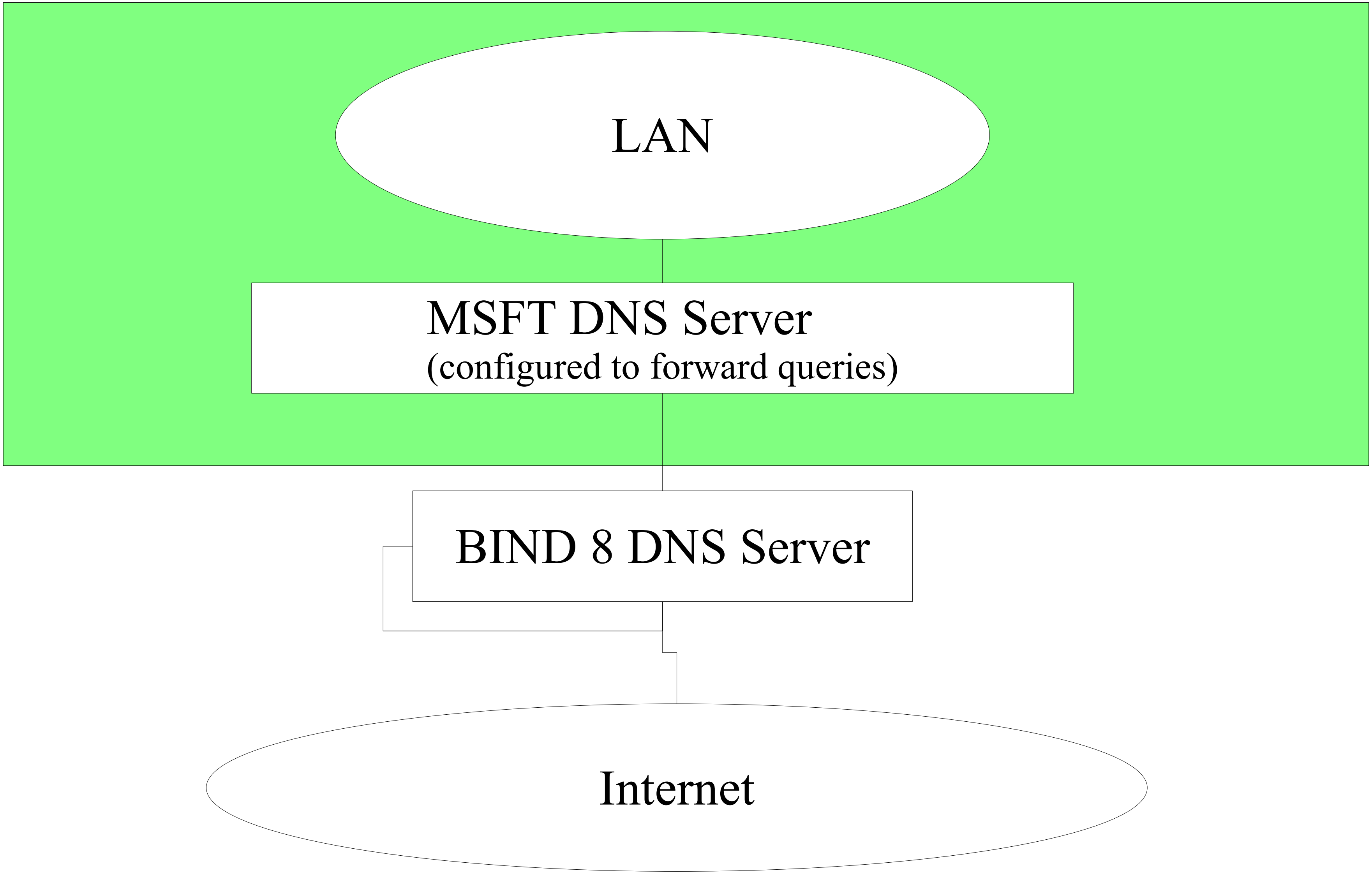
April 4th:

One month after initial reports, the problem still persists. We raise the infocon level to “Yellow” to solicit more information.

April 5th:

Information that some MSFT products may be vulnerable.

MSFT – BIND Interaction



MSFT – BIND Part 2

- MSFT DNS server configured to forward queries to trusted external DNS server.
  - Isolates internal DNS server from attacks.
  - May increase performance.
  - Simplifies firewall setup.
- BIND 8 will not clean responses it passes to the internal (MSFT) DNS Server.
- The MSFT DNS server will now trust the responses it receives, even though they still include the malicious content.

DNS Poisoning – Resolution

- Solution: Upgrade to BIND 9.
- Further analysis: One of our handlers did manage to get a hold of the DNS server which was the origin of the poisoning. The poisoning was achieved using a standard configuration of BIND:
  - Configure a .com zone, and make the DNS server authoritative.
  - Setup wildcard records for the .com zone.
- Based on old zone files / comments we see that at each time, two IP addresses where used. These where changed frequently.

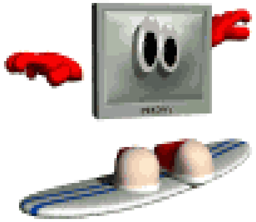
Future Outlook / Trends

- Client Exploits.
  - Cognitive exploits (phishing)
  - Web browser Exploits.

(malware spiders, “honey monkey”)

- ~~Commercialization.~~
- Secondary server application exploits.
  - PHPBB.
  - awstats. (collecting web logs)
- AV is dead. There is no new malware, just new packers. (malware analysis effort, automated pattern matching for packers)

Q & A



URLs of interest:

Internet Storm Center: http://isc.sans.org

DShield: http://www.dshield.org

How to send logs: http://www.dshield.org/howto.php

SANS Webcasts: http://www.sans.org/webcasts.php

! THANKS !

¡GRACIAS!